UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THOMAS BOOTH HARRIS, on behalf of himself and all others similarly situated, Plaintiff, v. SOMNIA, INC. and PALM SPRINGS ANESTHESIA SERVICES, P.C., Defendants.	Case No. 22-9550 **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Thomas Booth Harris, through his attorneys, bring this Class Action Complaint against the Defendants Somnia, Inc. ("Somnia") and Palm Springs Anesthesia Services, P.C. ("PSAS") and collectively ("Defendants") alleges as follows:

INTRODUCTION

1. Defendant Somnia, a practice management company for anesthesia providers and clinics across the country, lost control over highly sensitive personal information stored in its computer system in a July 2022 data breach by cybercriminals ("Data Breach").

2. Upon information and belief, Defendant PSAS, a provider of anesthetic services with an office in Palm Springs, California, contracts with Somnia to manage PSAS' business and gives Somnia access to PSAS' highly sensitive patient information.

3. On or around July 11, 2022, Somnia detected suspicious activity in its computer systems. On information and belief, cybercriminals were able to pilfer the sensitive and confidential personally identifiable information ("PII") and protected health information ("PHI") belonging to over 386,000 consumers.

4. The stolen PII and PHI included names, Social Security numbers, dates of birth,

driver's license numbers, financial account information, health insurance policy number, medical record numbers, Medicaid and Medicare identification numbers and health information such as treatment and diagnosis information.

5. PSAS's patient information was among the PII and PHI that was stolen in the Data Breach.

6. After discovering the Data Breach in July 2022, Somnia and PSAS waited more than three (3) months to alert the victims about the Data Breach. A copy of the Data Breach notice (the "Breach Notice") is attached hereto as **Exhibit A.**

7. The unreasonable delay between detection of the Data Breach and providing notice left impacted patients in the dark, with no means to prevent or stop cybercriminals from using their PII and PHI.

8. Defendants are well-aware of their duty to protect sensitive PII and PHI. Somnia's website states, "SOMNIA, INC. takes its users' privacy concerns seriously." https://somniaanesthesiaservices.com/legal/privacy-policy/ (last visited November 3, 2022). Somnia acknowledges "the importance of responsible use of Personal Information collected." *Id*.

9. By entrusting its patient PII and PHI with Somnia, PSAS had a duty to ensure Somnia was appropriately safeguarding this highly sensitive patient information.

10. PSAS failed in that regard. PSAS acknowledges in the Data Breach Notice that Somnia's security measures were not sufficient. In fact the Data Breach Notice cites improvements Somnia must implement to protect patient PII and PHI going forward:

What Are We Doing?

The management company has assured us that they have taken steps to prevent a similar incident in the future, including conducting a global password reset, tightening firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers.

11. On information and belief, Defendants failed in their respective duties to protect

PII and PHI from unauthorized disclosure because Somnia did not implement or adhere to cybersecurity measures that would have prevented or stopped cybercriminals from accessing PII and PHI, and PSAS failed to ensure such measures were followed.

12. Defendants' negligent conduct puts Plaintiff and other current and former patients at risk.

13. Armed with patient PII and PHI obtained from Somnia and PSAS, data thieves can commit various crimes including, e.g., opening new financial accounts in consumers' names, taking out loans in consumers' names, using consumers' names to obtain medical services, using consumers' information to obtain government benefits, filing fraudulent tax returns using consumers' information, obtaining driver's licenses in consumers' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Defendants' current and former patients have been exposed to a heightened and imminent risk of fraud and identity theft. They must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Consumers also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

18. Plaintiff, Thomas Booth Harris, is a natural person and citizen of California, residing in California, where he intends to remain. Plaintiff Thomas Booth Harris is a Data Breach victim and received electronic notice of the Breach Notice on October 28, 2022.

19. Defendant Somnia is a New York corporation, with its principal place of business at 450 Mamaroneck Ave., Suite 201, Harrison, New York, 10528.

20. Defendant PSAS is a California corporation with its principal place of business at 450 Mamaroneck Ave., Suite 201, Harrison, New York, 10528.

JURISDICTION & VENUE

21. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

22. This Court has personal jurisdiction over Defendants because their respective principal places of business are in this District, and Defendants do substantial business in this District.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

a. Defendants

24. Defendant Somnia is a practice management company that works with anesthesia departments in hospitals, surgery centers and medical offices across the country.

25. Upon information and belief, Defendant PSAS is a medical group comprised of

approximately 80 health care providers who provide anesthesia services to medical offices in California including in Palm Springs, Camarillo, Long Beach, Oxnard, San Bernardino and Stockton, California.

26. Upon information and belief PSAS contracts with Somnia for practice management services and, in the course of that relationship, shares its patients' PII and PHI with Somnia.

b. Defendants Fail to Safeguard Patient PII and PHI

27. Plaintiff Booth Harris had surgery in December 2021 at St. John's Hospital Smarillo in Camarillo, California, and was placed under anesthesia. Upon information and belief, PSAS health providers performed healthcare services related to Plaintiff's surgery and thereby obtained Plaintiff's PII and PHI.

28. As a condition of receiving healthcare services, patients using healthcare providers who contract with Somnia for practice management were required to disclose their PII and PHI.

29. Defendants collect and maintain patient and former patient PII and PHI in their computer systems.

30. In collecting and maintaining the PII and PHI, Defendants agreed they would safeguard the data according to internal policies and state and federal law.

31. Even so, on or about July 11, 2022, Somnia learned hackers had bypassed its security systems and accessed patient PII and PHI.

32. Hackers did so undetected and neither Somnia nor PSAS has disclosed how long hackers had access to their patient PII and PHI.

33. By the time cybersecurity experts discovered the Data Breach, cybercriminals had already accessed patients' PII and PHI including their names, Social Security numbers, dates of birth, driver's license numbers, financial account information, health insurance policy number,

medical record numbers, Medicaid and Medicare identification numbers and health information such as treatment and diagnosis information.

34. After discovering the breach, the Breach Notice says Somnia "implemented its incident response protocols," but the Breach Notice does not state whether the Data Breach was contained immediately, nor does it disclose how long the Data Breach went undetected.

35. Upon information and belief, cybercriminals could breach Defendants' systems because Defendants failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patient PII and PHI. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing PHI and PII. Further, the Breach Notice makes clear that Defendants cannot, or will not, determine the full scope of the Data Breach, as they have been unable to determine exactly what information was stolen and when.

c. Plaintiff's Experience

36. Plaintiff has no known relationship with the Defendants other than that he had surgery in December 2021 in a California location under anesthesia and received a Breach Notice.

37. As a condition of Plaintiff obtaining healthcare services from PSAS, Plaintiff was required to provide his PII and PHI.

38. Plaintiff provided his PII and PHI to Defendants and trusted they would use reasonable measures to protect it according to Defendants' internal policies and state and federal law.

39. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Breach Notice and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This

time has been lost forever and cannot be recaptured.

40. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII and PHI was exposed in the Data Breach.

41. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

42. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII and PHI—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

43. Plaintiff has suffered present, continuing, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

44. Plaintiff has a continuing interest in ensuring that his PII and PHI (still in Defendants' possession) is protected and safeguarded from future breaches.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

45. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendants.

46. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII and PHI in their possession.

47. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to $1,000.00 depending on the type of information obtained.

48. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

49. It can take victims years to spot identity or PII/PHI theft, giving criminals plenty of time to use that information for cash.

50. One such example of criminals using PII and PHI for profit is the development of

"Fullz" packages.

51. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

52. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is traceable to the Data Breach.

53. Defendants disclosed the PII and PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII and PHI of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

54. For healthcare providers, data breaches entail a particularly severe, foreseeable risk of harm. According to the American Medical Association, "cyberattacks not only threaten the

privacy and security of patients' health and financial information, but also patient access to care."[1] And the risk of identity theft carries serious implications for data breach victims: "an increased risk of identity theft is akin to the risk of contracting a chronic disease.

55. The risk of a data breach is ongoing. Data-breach notification letters often explicitly inform people that there is a risk of identity theft. Credit-monitoring services are generally offered for one or two years, signaling to victims an increased risk of theft for that time.

56. When a person has a reasonable belief that her credit identity is in jeopardy, she is rightly afraid that her creditworthiness is out of her hands. The exposure to the risk of identity theft can be anxiety-inducing because identity theft can have catastrophic effects on an individual's life and because it is difficult to resolve. The passage of time may not dissipate that fear because identity theft can happen at any time. A person's financial and employment opportunities can be destroyed by identity theft, and time and money are essential to addressing it. In all these ways, identity theft is the digital equivalent to contracting a chronic disease."[2]

57. Defendants' failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendants failed to adhere to FTC guidelines.

58. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous

[1] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited November 4, 2022)
[2] Daniel J. Solove & Danielle K. Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 762 (2018) (footnotes omitted).

guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PII.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

60. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

61. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

f. Defendants fail to protect Plaintiff's PHI

64. When it comes to a breach of PHI, the injury and the harm *has already occurred*. No further disclosure is necessary. As Justice Brandeis once observed, invasions of privacy are themselves concrete injuries and, indeed, can subject victims "to mental pain and distress, far greater than could be inflicted by mere bodily injury."[3]

65. Medical data breaches acutely implicate the right to privacy, as "[p]atients are highly sensitive to disclosure of their health information," particularly because PHI "often involves intimate and personal facts, with a heavy emotional overlay."[4]

66. Unsurprisingly, then, empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of American patients express concern about the privacy of their medical records."[5]

67. Plaintiff and the Class had a reasonable expectation of privacy in their PHI.

68. The disclosure of PHI is highly offensive to a reasonable person.

69. As a direct and proximate result of Defendants' acts and omissions, Plaintiff and the Class suffered harm, an invasion of privacy, when their PHI was viewed by an unauthorized third-party.

70. HIPAA circumscribes security provisions and data privacy responsibilities

[3] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).
[4] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002).
[5] Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKLEY TECH. L.J. 1523, 1557 (2009).

designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

71. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

72. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

CLASS ACTION ALLEGATIONS

73. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class") and California subclass ("Subclass") (together "Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose PII and PHI was compromised in the Data Breach.
>
> **California Subclass**: All individuals residing in California whose PII and PHI was compromised in the Data Breach.

Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors or assigns, and any Judge who adjudicates this case, including their staff and immediate family.

74. Plaintiff reserves the right to amend the class definitions.

75. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of at least 385,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interest does not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII and PHI;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's PII and PHI;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

76. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

77. Plaintiff realleges all previous paragraphs as if fully set forth below.

78. Plaintiff and members of the Class entrusted their PII and PHI to Defendants. Defendants owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized

access.

79. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII and PHI—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

80. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

81. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and members of the Class's PII and PHI.

82. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendants holds vast amounts of PII and PHI it was

inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII and PHI—whether by malware or otherwise.

83. PII and PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

84. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

85. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se

(On Behalf of Plaintiff and the Class)

86. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

87. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

88. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII and PHI.

89. Defendants are entities covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

90. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtain and store, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

91. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

92. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's sensitive PII.

93. Defendants violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect their patients' PII and PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

94. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

95. Defendants had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

96. Defendants breached their respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII and PHI.

97. Defendants' violation of HIPAA and Section 5 of the FTCA and its failure to comply with applicable laws and regulations constitutes negligence per se.

98. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff

and members of the Class, Plaintiff and members of the Class would not have been injured.

99. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

100. Had Plaintiff and members of the Class known that Defendants did not adequately protect their PII and PHI, Plaintiff and members of the Class would not have entrusted Defendants with their PII and PHI.

101. As a direct and proximate result of Defendants' negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Violations of the Confidentiality of Medical Information Act,
CAL. CIV. CODE § 56, *et seq.*
(On behalf of Plaintiff and the California Subclass)

102. Plaintiff incorporates by reference all preceding allegations.

103. Under Section 56.101, "[a]ny provider of health care . . .or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." (CAL. CIV. CODE § 56.101, subdiv. a.) Section 56.36(b) provides that "an

individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both" actual damages and nominal damages of $1,000. (CAL. CIV. CODE § 56.36, subdiv. b.)

104. A claim for "negligent release under section 56.36 does not require an affirmative communicative act but instead can be accomplished by negligently allowing information to end up in the possession of an unauthorized person." (*Sutter Health v. Superior Court* (2014) 227 Cal. App. 4th 1546, 1554–55.) Defendants are liable if their "negligence results in unauthorized or wrongful access to the [plaintiff's] information." (*Regents of Univ. of Cal. v. Superior Court* (2013) 220 Cal. App. 4th 549, 554.)

105. Defendants created, maintained, preserved, stored, abandoned, destroyed, and disposed of medical information regarding Plaintiff and the Class.

106. Defendants were negligent because they failed to take reasonable precautions to ensure their data systems were protected.

107. As a result of Defendants' negligence, an unauthorized third-party gained wrongful access to the medical information of Plaintiff and the Class.

108. Defendants are therefore liable for damages in an amount to be determined at trial, but not less than the statutorily provided nominal damages of $1,000 for each class member.

COUNT IV:
Violations of the Consumer Records Act,
CAL. CIV. CODE § 1798.80, *et seq.*
(On behalf of Plaintiff and the California Subclass)

109. Plaintiff incorporates by reference all preceding allegations.

110. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the

data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (CAL. CIV. CODE § 1798.2.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (CAL. CIV. CODE § 1798.82, subdiv. b.)

111. The Data Breach constitutes a "breach of the security system" of Defendants.

112. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

113. Defendants knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class, but waited more than three (3) months to notify them.

114. Three months was an unreasonable delay under the circumstances.

115. Defendants' unreasonable delay prevented Plaintiff from taking appropriate measures from protecting himself against harm.

116. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

117. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT V
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff and the California Subclass)

118. Plaintiff incorporates by reference all preceding allegations.

119. Defendants violated § 1798.150 of the CCPA by failing to implement and maintain

reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the California Subclass. As a direct and proximate result, Plaintiff's and the California Subclass's PII and PHI was subject to unauthorized access and exfiltration, theft, or disclosure.

120. Defendants are a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

121. Plaintiff and California Subclass members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard PII and PHI by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold PII and PHI, including Plaintiff's and California Subclass members' PII and PHI. Plaintiff and California Subclass members have an interest in ensuring that their PII and PHI is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

122. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendants' registered service agents, detailing the specific provisions of the CCPA that Defendants have violated and continue to violate. If Defendants cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

123. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

124. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants.

COUNT VI:
Violations of the Unfair Competition Law,
BUS. & PROF. CODE § 17200, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

125. Plaintiff incorporates by reference all preceding allegations.

126. The Unfair Competition Law provides that:

> "[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." (BUS. & PROF. CODE § 17200.)

127. Defendants stored the PII and PHI of Plaintiff and the Class in their computer systems and knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII and PHI secure and prevented the loss or misuse of that information.

128. Defendants failed to disclose to Plaintiff and the Class that their PII and PHI was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendants had secured their PII and PHI. At no time were Plaintiff and the Class on notice that their PII and PHI was not secure, which Defendants had a duty to disclose.

129. Had Defendants complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

130. Defendants' conduct was unlawful, in that it violated the CMIA, CRA, and CCPA.

131. Defendants' conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

132. Defendants also engaged in unfair business practices under the "tethering test."

Their actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

133. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

134. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

135. There were reasonably available alternatives to further Defendants' legitimate business interests, other than the misconduct alleged in this complaint.

136. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendants; disgorgement of all profits accruing to Defendants because of its unfair and improper business practices; a permanent injunction enjoining Defendants' unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VII
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Class)

137. Plaintiff incorporates all previous paragraphs as if fully set forth below.

138. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

139. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

140. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed, and continue to owe, a legal duty to employ reasonable data security to secure the PII and PHI with which they are entrusted, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendants breached, and continue to breach, their duty by failing to employ reasonable measures to secure patients' PII and PHI; and

c. Defendants' breach of their legal duty continues to cause harm to Plaintiff and the Class.

141. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to patients' PII and PHI.

142. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

143. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued.

144. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 8th day of November, 2022.

/s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
T: (212) 558-5500
F: (212) 344-5461
jbilsborrow@weitzlux.com

Samuel J. Strauss (*pro hac vice* forthcoming)
Raina C. Borrelli (*pro hac vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff